

JP11234264

===== WPI =====

TI - Electronic watermark system for electronic information distributing system - multiplies random number in portion of encryption lock and enables user to choose one of encryption keys, corresponding to encryption informations, and transmitted encryption information

AB - JP11234264 NOVELTY - A random number is multiplied in a portion of an encryption lock. A user chooses one of the encryption keys, corresponding to encryption informations, and a transmitted encryption information. The encryption keys and the encryption informations are transmitted to the user by a server. DETAILED DESCRIPTION - The encryption key is generated by performing the encryption of a predetermined encryption key using another predetermined encryption key. The encryption information is generated by performing the encryption of for every generated information using the predetermined encryption key. INDEPENDENT CLAIMS are also included for the following: an electronic information distributing system; and a memory medium.

- USE - For electronic information distributing system. Used for protecting copyright of digital information, e.g. moving image data, still picture image data, audio data, computer data, computer program, which is distributed in a multimedia network.

- ADVANTAGE - Prevents making a reverse process of the encryption key and a random number. Prevents a server from embedding user information freely and distributing the user information unjustly. Increases the operating efficiency of the electronic watermark system. Prevents inaccurate distribution of digital data. DESCRIPTION OF DRAWING(S) - The figure shows a diagram explaining an implanting process.

- (Dwg.1/8)

PN - JP11234264 A 19990827 DW199945 H04L9/36 015pp

PR - JP19980034770 19980217

PA - (CANO) CANON KK

MC - T01-H01C2 T03-P01 W01-A05 W02-J03A2B W03-A W04-F

DC - P85 T01 T03 W01 W02 W03 W04

IC - G06F12/14 ;G09C5/00 ;G11B20/10 ;H04L9/36 ;H04N1/387 ;H04N5/91 ;H04N7/08 ;H04N7/081

AN - 1999-535482 [45]

Random number as w/m?
Notth about renewal / insertion
not perceptible?

TI - ELECTRONIC PAPERMARKING SYSTEM, ELECTRONIC INFORMATION DISTRIBUTION SYSTEM USING THE SAME AND STORAGE MEDIUM

AB - PROBLEM TO BE SOLVED: To surely prevent an illegal use of digital data and to decrease the amount of communication or calculation to be performed for preventing the illegal use.

- SOLUTION: This is an electronic papermarking system wherein a server performs a first processing for generating plural pieces of different electronic papermark information, a second processing for generating plural pieces of enciphered information by enciphering these plural pieces of information while using individual cryptographic keys for each piece, a third processing for generating plural enciphered cryptographic keys by enciphering these individual cryptographic keys by multiplying a random number and a fourth processing for transmitting the plural pieces of enciphered information and the plural enciphered cryptographic keys as mentioned above to a user, while a user performs a fifth processing for selecting one of the plural pieces of transmitted enciphered information or one of the plural enciphered cryptographic keys corresponding to the enciphered information. A safe and highly efficient system concerning the illegal distribution of digital data can be provided by multiplying the random number only to the partial cryptographic key when multiplying the random number to the individual cryptographic keys.

PN - JP11234264 A 19990827

PD - 1999-08-27

ABD - 19991130

ABV - 199913

AP - JP19980034770 19980217

PA - CANON INC

IN - IWAMURA KEIICHI

I - H04L9/36 ;G06F12/14 ;G09C5/00 ;G11B20/10 ;H04N1/387 ;H04N5/91 ;H04N7/08 ;H04N7/081

(51) Int.Cl. ⁸	識別記号	FI
H 0 4 L 9/36		H 0 4 L 9/00 6 8 5
G 0 6 F 12/14	3 2 0	G 0 6 F 12/14 3 2 0 E
G 0 9 C 5/00		G 0 9 C 5/00
G 1 1 B 20/10		G 1 1 B 20/10 H
H 0 4 N 1/387		H 0 4 N 1/387

審査請求 未請求 請求項の数22 O L (全 15 頁) 最終頁に続く

(21) 出願番号 特願平10-34770

(22) 出願日 平成10年(1998) 2月17日

(71) 出願人 000001007

キヤノン株式会社

東京都大田区下丸子3丁目30番2号

(72) 発明者 岩村 恵市

東京都大田区下丸子3丁目30番2号 キヤ
ノン株式会社内

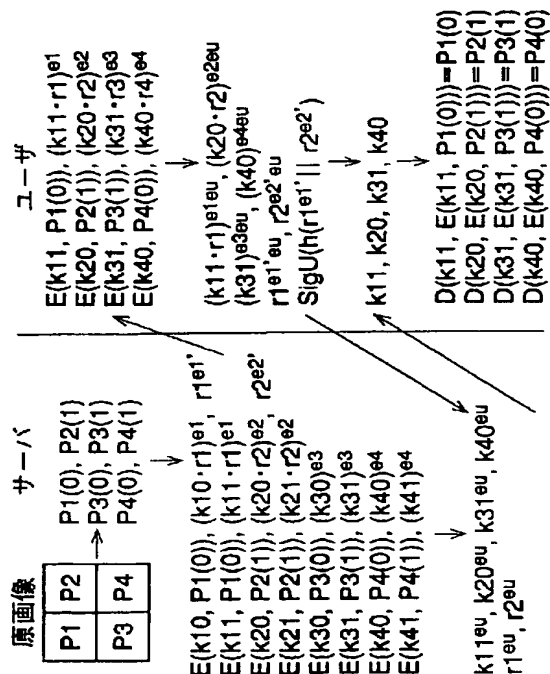
(74) 代理人 弁理士 國分 孝悦

(54) 【発明の名称】 電子透かし方式及びそれを用いた電子情報配布システム並びに記憶媒体

(57) 【要約】

【課題】 デジタルデータが不正に使用されるのを確実に防止できるようにするとともに、不正使用を防止するために行う通信量や計算量を減少できるようにする。

【解決手段】 電子透かし情報の異なる複数の情報を生成する第1の処理と、上記複数の情報毎に個別の暗号鍵を用いて暗号化して複数の暗号化情報を生成する第2の処理と、上記個別の暗号鍵に乱数を乗じて暗号化して複数の暗号化暗号鍵を生成する第3の処理と、上記複数の暗号化情報および暗号化暗号鍵をユーザに送信する第4の処理とをサーバが行い、上記送信された複数の暗号化情報や上記暗号化情報に対応する暗号化暗号鍵の1つを選択する第5の処理を上記ユーザが行う電子透かし方式において、上記個別の暗号鍵に乱数を乗じる際に、一部の暗号鍵にのみ乱数を乗じることにより、デジタルデータの不正配布に関して安全で高効率なシステムを実現できるようにする。



【特許請求の範囲】

【請求項1】 電子透かし情報の異なる複数の情報を生成する第1の処理と、上記複数の情報毎に個別の暗号鍵を用いて暗号化して複数の暗号化情報を生成する第2の処理と、上記個別の暗号鍵を別の暗号鍵を用いて暗号化して複数の暗号化暗号鍵を生成する第3の処理と、上記複数の暗号化情報および暗号化暗号鍵をユーザに送信する第4の処理とをサーバが行い、上記送信された複数の暗号化情報や上記暗号化情報に対応する暗号化暗号鍵の1つを選択する第5の処理を上記ユーザが行う電子透かし方式において、
上記暗号鍵の一部にのみ乱数を乗じることを特徴とする電子透かし方式。

【請求項2】 上記サーバは乱数を暗号化して暗号化乱数を生成し、上記暗号化乱数を保存するとともに、ユーザに送信することを特徴とする請求項1に記載の電子透かし方式。

【請求項3】 上記電子透かしの正当性を検証する処理を行うことを特徴とする請求項1または2に記載の電子透かし方式。

【請求項4】 電子透かしの正当性を検証する処理を繰り返して行うことを特徴とする電子透かし方式。

【請求項5】 電子透かし処理により埋め込まれたユーザに対応する電子透かし情報の正当性を暗号化処理を用いて保証するようにした電子透かし方式において、
上記ユーザの電子透かし情報を検査する処理を行うことを特徴とする電子透かし方式。

【請求項6】 上記ユーザの署名を認証局による証明書付き匿名公開鍵によって検査する処理を行うことを特徴とする請求項1～5の何れか1項に記載の電子透かし方式。

【請求項7】 上記暗号化処理及び／または電子透かし埋め込み処理を検査するための情報をヘッダ部に有する画像フォーマットを用いることを特徴とする請求項1～6の何れか1項に記載の電子透かし方式。

【請求項8】 画像属性情報および画像データを構造化して画像ヘッダ部に格納した画像フォーマットであって、上記請求項1～6の何れか1項に記載の暗号化処理及び／または電子透かし埋め込み処理を検査するための検査情報を上記画像属性情報として有する画像フォーマットを用いることを特徴とする請求項1～6の何れか1項に記載の電子透かし方式。

【請求項9】 請求項1～6の何れか1項に記載の電子透かし方式の手順をコンピュータに実行させるためのプログラムを格納したことを特徴とする記憶媒体。

【請求項10】 上記暗号化処理及び／または電子透かし埋め込み処理を検査するための情報をヘッダ部に有する画像フォーマットを格納したことを特徴とする記憶媒体。

【請求項11】 画像属性情報および画像データを構造

化して画像ヘッダ部に格納した画像フォーマットを格納した記憶媒体において、

上記請求項1～5の何れか1項に記載の暗号化処理及び／または電子透かし埋め込み処理を検査するための検査情報を上記画像属性情報として有する画像フォーマットを格納したことを特徴とする記憶媒体。

【請求項12】 電子透かし情報の異なる複数の情報を生成する第1の手段と、上記複数の情報毎に個別の暗号鍵を用いて暗号化して複数の暗号化情報を生成する第2の手段と、上記個別の暗号鍵を別の暗号鍵を用いて暗号化して複数の暗号化暗号鍵を生成する第3の手段と、上記複数の暗号化情報および暗号化暗号鍵をユーザに送信する第4の手段とをサーバが有し、上記送信された複数の暗号化情報や、上記暗号化情報に対応する暗号化暗号鍵の1つを選択する第5の手段をユーザが有する電子情報配付システムにおいて、

上記暗号鍵の一部にのみ乱数を乗じるようにする第6の手段をサーバに設けたことを特徴とする電子情報配付システム。

【請求項13】 上記サーバは乱数を暗号化して暗号化乱数を生成し、上記暗号化乱数を保存するとともに、ユーザに送信する第7の手段を更に有することを特徴とする請求項12に記載の電子情報配付システム。

【請求項14】 上記電子透かしの正当性を検証する第8の手段をさらに有することを特徴とする請求項12または13に記載の電子情報配付システム。

【請求項15】 電子透かしの正当性を検証する処理を繰り返して行うようにしたことを特徴とする電子情報配付システム。

【請求項16】 電子透かし処理により埋め込まれたユーザに対応する電子透かし情報の正当性を暗号化処理を用いて保証するようにした電子情報配付システムにおいて、
上記ユーザの電子透かし情報を検査する検査手段を有することを特徴とする電子情報配付システム。

【請求項17】 上記ユーザの署名を認証局による証明書付き匿名公開鍵によって検査する検査手段をさらに有することを特徴とする請求項12～16の何れか1項に記載の電子情報配付システム。

【請求項18】 上記暗号化処理及び／または電子透かし埋め込み処理を検査するための検査情報をヘッダ部に有する画像フォーマットを用いることを特徴とする請求項12～16の何れか1項に記載の電子情報配付システム。

【請求項19】 画像属性情報および画像データを構造化して画像ヘッダ部に格納した画像フォーマットであって、上記請求項12～16の何れか1項に記載の暗号化処理及び／または電子透かし埋め込み処理を検査するための検査情報を上記画像属性情報として有する画像フォーマットを用いることを特徴とする請求項12～16の

何れか1項に記載の電子情報配付システム。

【請求項20】 請求項12～16の何れか1項に記載の各手段としてコンピュータを機能させるためのプログラムを格納したことを特徴とする記憶媒体。

【請求項21】 上記暗号化手段により行われる暗号化処理及び／または電子透かし埋め込み手段により行われる電子透かし埋め込み処理を検査するための検査情報をヘッダ部に有する画像フォーマットを格納したことを特徴とする記憶媒体。

【請求項22】 画像属性情報および画像データを構造化して画像ヘッダ部に格納した画像フォーマットを格納した記憶媒体において、

上記請求項12～16の何れか1項に記載の暗号化手段により行われる暗号化処理及び／または電子透かし埋め込み手段により行われる電子透かし埋め込み処理を検査するための検査情報を上記画像属性情報として有する画像フォーマットを格納したことを特徴とする記憶媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は電子透かし方式及びそれを用いた電子情報配布システム並びに記憶媒体に関し、特に、動画像データ、静止画像データ、音声データ、コンピュータデータ、コンピュータプログラム等のデジタル情報における著作権を保護するための電子透かし技術、及びそれを用いてデジタル情報の配布を行うマルチメディアネットワークに用いて好適なものである。

【0002】

【従来の技術】近年のコンピュータネットワークの発達と、安価で高性能なコンピュータの普及とにより、ネットワーク上で商品の売買を行う電子商取引が盛んになってきている。上記ネットワーク上で取引される商品として、画像等を含むデジタルデータが考えられる。

【0003】しかし、デジタルデータは完全なコピーを容易に、かつ大量に作成できるという性質を有しているので、そのデジタルデータを買ったユーザがオリジナルと同質のコピーを不正に作成して再配付することができるという可能性を持っている。デジタルデータが不正に作成されて再配布されてしまうと、本来は著作者または著作者から正当に販売を委託された者（販売者）に支払われるべき代価が支払われず、著作権が侵害されてしまう恐れがある。

【0004】一方、著作者または販売者（以後、デジタルデータを正当に配布する者をサーバと呼ぶ）がデジタルデータを1度ユーザに送ってしまうと、上記の不正コピーを完全に防止することはできない。そこで、不正コピーを直接防止するのではなく、電子透かしと呼ばれ、著作権の保護に役立つ手法が提案されている。

【0005】上記電子透かしとは、オリジナルのデジタルデータにある操作を加え、デジタルデータに関する

著作権情報やユーザに関する利用者情報をデジタルデータ中に埋め込むことによって、不正コピーが見つかった場合にデジタルデータを誰が再配布したのかを特定するための手法である。

【0006】電子透かしを用いる従来のシステムでは、サーバは完全に信頼できる機関であることが前提となっている。このため、サーバが信頼できる機関ではなく不正を行う可能性があるとする、従来のシステムでは不正コピーを行っていないユーザに罪が押し付けられてしまう恐れがある。

【0007】これは、従来の電子透かしを用いるシステムは、サーバがユーザを特定するために用いる利用者情報をデジタルデータ（以後、デジタルデータを画像データとして説明する）に埋め込むので、サーバが勝手に利用者情報を埋め込みそのコピーを不正に配布した場合、その利用者情報から特定されるユーザは、サーバの主張を退ける手段がないためである。その対策として、いくつかの手法が提案されている。例えば、図4に示したような手法が提案されている。

【0008】〔埋め込み処理〕図4に示した手法は、先ず、第1の埋め込み処理として、サーバは、原画像をN個のブロックに分割し、各ブロックを P_n ($n=1, \dots, N$)とおく。次に、各ブロック P_n を N_s 個 ($N_s < N$)のSブロックと、 N_u 個 ($N_u = N - N_s$)のUブロックとに分ける。

【0009】図4では、原画像を4分割し、上側のブロック P_1 、 P_2 をSブロックとし、下側のブロック P_3 、 P_4 をUブロックとしている。また、サーバは暗号鍵 k によってデータ P を暗号化する暗号化手段 $E(k, P)$ を準備する。

【0010】一方、ユーザは、それに対応する復号手段を持つ。また、サーバとユーザは独立に「 $e \cdot d = 1 \pmod{p-1}$ 」となる変数 e と d を生成する。ただし、 $p = 2q + 1$ [q は素数]であり、サーバは以上のような変数 e と d を $2 \cdot N$ 組生成し、 (e_n, d_n) とおく（ユーザの e と d は e_u, d_u とおく）。

【0011】次に、第2の埋め込み処理として、サーバは、Sブロックにユーザ毎に定めたユーザ情報を埋め込み、Uブロックの複製を 2^b 個生成して $0 \sim 2^b - 1$ の数値を埋め込む。以降、ブロック P_n に数値 i が埋め込まれた時それを $P_n(i)$ と表現する。

【0012】図4では、Sブロックである P_1 、 P_2 にユーザ情報として $\{0, 1\}$ が埋め込まれ、 $b=1$ としてUブロックである P_3 、 P_4 の2個の複製に対して0と1の数値が埋め込まれている。

【0013】次に、第3の埋め込み処理として、サーバは、Sブロックの $P_n(i)$ の複製を 2^b 個生成し、各々異なる暗号鍵 k_{nj} ($j=0, \dots, 2^b - 1$)で暗号化した $E(k_{nj}, P_n(i))$ と、暗号鍵 k_{nj} に乱数 r_n をかけて e_n で暗号化した $(k_{nj} \cdot r_n)^{e_n}$ を

ともにユーザに送る。さらに、 $Nu \cdot 2^b$ 個のUブロック $Pn(i)$ を各々 kni で暗号化した $E(kni, Pn(j))$ と暗号鍵 kni に乱数 rn をかけて en で暗号化した $(kni \cdot rn)^{en}$ をともにユーザに送る。

【0014】また、サーバは乱数 rn を en' ($n' = N+n$) で暗号化した暗号化乱数 rn^{en} を保存し、かつユーザに送る。以後、暗号化手段 $E(k, P)$ によって暗号化した画像を暗号化画像、暗号鍵に乱数をかけて en で暗号化したものをサーバ暗号化暗号鍵、また en' で暗号化した乱数をサーバ暗号化乱数と呼ぶ。このとき、暗号化画像やサーバ暗号化暗号鍵、サーバ暗号化乱数はその対応が正しければランダムに送ることができる。

【0015】次に、第4の埋め込み処理として、ユーザは、送られてきた複数の暗号化画像とサーバ暗号化暗号鍵のペアの中から各ブロック毎に1つずつのペアを選ぶ。図4では、各ブロック毎に $E(k11, P1(0))$ ($k11 \cdot r1$)^{e1}、 $E(k20, P2(1))$ ($k20 \cdot r2$)^{e2}、 $E(k31, P3(1))$ ($k31 \cdot r3$)^{e3}、 $E(k40, P4(0))$ ($k40 \cdot r4$)^{e4} を選んだことになる。

【0016】次に、第5の埋め込み処理として、ユーザは、選んだサーバ暗号化暗号鍵とすべてのサーバ暗号化乱数を自分の暗号鍵 eu で暗号化して、2重暗号化暗号鍵と2重暗号化乱数を生成してサーバに送る。

【0017】このとき、ユーザはすべてのサーバ暗号化乱数をつなぎ合わせた合成乱数等に対するハッシュ値に公開鍵暗号方式による署名を施してサーバに送る。これは、図4において、 $SigU(h(r1^{e1'} \parallel r2^{e2'} \parallel r3^{e3'} \parallel r4^{e4'}))$ で表される。

【0018】次に、第6の埋め込み処理として、サーバは、署名をユーザの公開鍵を用いて検査した後、送られてきた2重暗号化暗号鍵と2重暗号化乱数の復号を行う。すなわち、暗号鍵 en で暗号化されたデータに対して dn 乗をして mod をとる。

【0019】次に、復号した暗号化暗号鍵を、復号した暗号化乱数(ユーザ暗号化乱数)で割った結果(ユーザ暗号化暗号鍵)をユーザに送る。このとき、サーバは復号したSブロックのユーザ暗号化乱数とUブロックのユーザ暗号化暗号鍵と送られてきた署名を保存する。

【0020】図4では、これによって $k11^{eu}$ 、 $k20^{eu}$ 、 $k31^{eu}$ 、 $k40^{eu}$ がユーザに送られ、 $r1^{eu}$ 、 $r2^{eu}$ 、 $k31^{eu}$ 、 $k40^{eu}$ と $SigU(h(r1^{e1'} \parallel r2^{e2'} \parallel r3^{e3'} \parallel r4^{e4'}))$ がサーバに保存される。

【0021】次に、第7の埋め込み処理として、ユーザは、送られてきたユーザ暗号化暗号鍵を復号し、その復号された暗号鍵によって暗号化画像を復号し、分割された各ブロックを合成することによって電子透かし画像を得る。

【0022】図4では、送られたユーザ暗号化暗号鍵を復号する、すなわち、 du 乗して mod をとることによって暗号鍵 $k11$ 、 $k20$ 、 $k31$ 、 $k40$ を得ることができる。この鍵は、上記第4の埋め込み処理で選択した暗号化画像の暗号鍵となっているので、この鍵で暗号化画像を復号することにより、 $P1(0)$ 、 $P2(1)$ 、 $P3(1)$ 、 $P4(0)$ を得ることができる。

【0023】したがって、各ブロックを合成することによって、Sブロックにユーザ情報 $\{0, 1\}$ をもち、Uブロックにはユーザによって選択された $\{1, 0\}$ のパターンをもつ電子透かし画像が得られる。

【0024】この手法では、ユーザがUブロックにどの数値が埋め込まれたブロックを選択したかをサーバは知ることができないので、サーバによる電子透かし画像の不正配布を行うことができない。

【0025】不正ユーザの特定は、サーバが不正画像からそのユーザのUブロックの数値、またはUブロックを暗号化した鍵を検証者に対して示すことによって認定される。不正画像が発見された場合、例えば、文献「[BaBa, Iwamura, Zheng, Imai: 'An Interactive Protocol for Image Fingerprinting', SCIS98-10. 2. E]」では、検証処理は次のように行われる(図5参照)。

【0026】〔検証処理〕第1の検証処理として、サーバは、不正画像のSブロックからユーザ情報を取り出し、不正をしたと思われるユーザを特定する。次に、サーバは不正画像に基づいてUブロックにおいてユーザが選択した各々のブロックを特定し、そのブロックを暗号化した暗号鍵を特定する。サーバは、特定したユーザ名、及び保存しているSブロックのユーザ暗号化乱数とUブロックのユーザ暗号化暗号鍵と署名、さらに上記第3の埋め込み処理で保存したすべてのサーバ暗号化乱数と、Sブロックに用いた乱数と、特定したUブロックの暗号鍵を検証者に渡して、以降の検証処理を依頼する。よって、図5ではサーバは検証者にユーザ名他に「 $r1^{eu}$ 、 $r2^{eu}$ 、 $k31^{eu}$ 、 $k40^{eu}$ 、 $SigU(h(r1^{e1'} \parallel r2^{e2'} \parallel r3^{e3'} \parallel r4^{e4'}))$ 、 $r1^{e1}$ 、 $r2^{e2}$ 、 $r3^{e3}$ 、 $r1$ 、 $r2$ 、 $k31$ 、 $k40$ 」を送る。

【0027】次に、第2の検証処理として、検証者は、提出されたサーバ暗号化乱数からハッシュ値を生成し、ユーザの公開鍵を用いて署名を検査し、一致するかどうか検査する。上記検査の結果が一致しない場合、そのサーバ暗号化乱数はそのユーザへの埋め込み処理に用いられたものではないので、ユーザは不正していないと認定される。

【0028】すなわち、 $r1^{e1'}$ 、 $r2^{e2'}$ 、 $r3^{e3'}$ 、 $r4^{e4'}$ からハッシュ値 $h(r1^{e1'} \parallel r2^{e2'} \parallel r3^{e3'} \parallel r4^{e4'})$ を生成し、署名 $SigU$

($h(r1^{e1'} \parallel r2^{e2'} \parallel r3^{e3'} \parallel r4^{e4'})$) をユーザの公開鍵で検査する。

【0029】次に、第3の検証処理として、検証者は、上記第1の埋め込み処理で用いられた $p (= 2q + 1)$ を基に N 組の異なる鍵を生成し、Sブロックの乱数とUブロックの暗号鍵を暗号化し、順番を変えてユーザに送る。

【0030】図5では、4組の暗号鍵 ($e1''$, $d1''$) ~ ($e4''$, $d4''$) が生成され、Sブロックの乱数 $r1$, $r2$ と、Uブロックの暗号鍵 $k31$, $k40$ を「 $r1^{e1''}$ 、 $r2^{e2''}$ 、 $r3^{e3''}$ 、 $r4^{e4''}$ 」と暗号化し、順序を逆にユーザに送っている。

【0031】次に、第4の検証処理として、ユーザは、送られてきたデータを埋め込み処理で用いた暗号鍵 eu によって暗号化してサーバに送る。図5では、「 $r1^{e1'' eu}$ 、 $r2^{e2'' eu}$ 、 $r3^{e3'' eu}$ 、 $r4^{e4'' eu}$ 」がサーバに送られる。ここで、Sブロックの乱数 $r1$, $r2$ とUブロックの暗号鍵 $k31$, $k40$ は順番が変えられているので、ユーザはSブロックとUブロックに属するブロックを識別できない。

【0032】次に、第5の検証処理として、サーバは、送られてきたデータを復号、すなわち、 di'' 乗して mod をとり、その結果を提出されたSブロックのユーザ暗号化乱数とUブロックのユーザ暗号化暗号鍵と比較する。

【0033】Sブロックのユーザ暗号化乱数が一致しない場合、ユーザが埋め込み処理と異なる鍵で上記第4の検証処理を行ったことになり、ユーザの不正と認定される。また、Sブロックのユーザ暗号化乱数が一致し、Uブロックのユーザ暗号化暗号鍵が一致した場合もユーザの不正と認定される。

【0034】それに対し、Sブロックのユーザ暗号化乱数が一致し、Uブロックのユーザ暗号化暗号鍵が一致しない場合のみユーザの不正と認定されない。よって、図5に示すように、Sブロックのユーザ暗号化乱数「 $r1^{eu}$ 、 $r2^{eu}$ 」とUブロックのユーザ暗号化暗号鍵「 $k31^{eu}$ 、 $k40^{eu}$ 」とを比較する。

【0035】

【発明が解決しようとする課題】上記の手法には、以下のような解決すべき問題点があった。第1の問題点として、Uブロックにおいて、暗号鍵と乱数の処理を逆にしても区別がつかないので、サーバはユーザに意図したUブロックの鍵を使用させることができる問題があった。

【0036】すなわち、図4において、 $E(k30, P3(0)) (k30 \cdot r3)^{e3}$ 、 $E(k31, P3(1)) (k31 \cdot r3)^{e3}$ 、 $r3^{e3'}$ の代わりに、 $E(k3, P3(0)) (k3 \cdot r30)^{e3}$ 、 $E(k3, P3(1)) (k3 \cdot r31)^{e3}$ 、 $k3^{e3'}$ としても、以後、同様の処理が可能である (P4 に関しても同様)。よって、サーバはユーザにUブロックに関して意

図した暗号鍵を使用させることができ、ユーザに罪を着せることが可能であった。

【0037】また、第2の問題点として、上記第4の検証処理における暗号鍵 eu を用いた暗号化において、ユーザがUブロックを暗号鍵 eu と異なる鍵で暗号化できれば、第5の検証処理においてUブロックのユーザ暗号化暗号鍵が異なるためにユーザの不正と認定されない。

【0038】しかし、第3の検証処理において、ユーザに送られる暗号化乱数と暗号化暗号鍵は並べ替えられているため、ユーザはUブロックの暗号化暗号鍵を特定できないことが上述の文献における安全性の根拠になっている。

【0039】しかし、不正画像の配布を行ったユーザが送られてきたデータの1つを暗号鍵 eu と異なる暗号鍵で暗号化して成功する確率は Nu/N である。理論的には、上記 N を何万という非常に大きな値とし、上記 Nu を一桁台の値とすれば、ある程度の安全性は実現できるが、毎回すべてのユーザに対して画像を何万ピクセルにも分解して上記の埋め込み処理を行うことは、通信量や計算量等を考えると実用的及び効率的ではなかった。

【0040】本発明は上述の問題点にかんがみ、デジタルデータが不正に使用されるのを確実に防止できるようにするとともに、不正使用を防止するために行う通信量や計算量を減少できるようにすることを目的とする。

【0041】

【課題を解決するための手段】本発明の電子透かし方式は、電子透かし情報の異なる複数の情報を生成する第1の処理と、上記複数の情報毎に個別の暗号鍵を用いて暗号化して複数の暗号化情報を生成する第2の処理と、上記個別の暗号鍵を別の暗号鍵を用いて暗号化して複数の暗号化暗号鍵を生成する第3の処理と、上記複数の暗号化情報および暗号化暗号鍵をユーザに送信する第4の処理とをサーバが行い、上記送信された複数の暗号化情報や上記暗号化情報に対応する暗号化暗号鍵の1つを選択する第5の処理を上記ユーザが行う電子透かし方式において、上記暗号鍵の一部にのみ乱数を乗じることを特徴としている。

【0042】また、本発明の電子透かし方式の他の特徴とするところは、上記サーバは乱数を暗号化して暗号化乱数を生成し、上記暗号化乱数を保存するとともに、ユーザに送信することを特徴としている。

【0043】また、本発明の電子透かし方式のその他の特徴とするところは、上記電子透かしの正当性を検証する処理を行うことを特徴としている。

【0044】また、本発明の電子透かし方式のその他の特徴とするところは、上記電子透かしの正当性を検証する処理を繰り返して行うことを特徴としている。

【0045】また、本発明の電子透かし方式のその他の特徴とするところは、電子透かし処理により埋め込まれたユーザに対応する電子透かし情報の正当性を暗号化処

理を用いて保証するようにした電子透かし方式において、上記ユーザの電子透かし情報を検査する処理を行うことを特徴としている。

【0046】また、本発明の電子透かし方式のその他の特徴とするところは、上記ユーザの署名を認証局による証明書付き匿名公開鍵によって検査する処理を行うことを特徴としている。

【0047】また、本発明の電子透かし方式のその他の特徴とするところは、上記暗号化処理及び／または電子透かし埋め込み処理を検査するための情報をヘッダ部に有する画像フォーマットを用いることを特徴としている。

【0048】また、本発明の電子情報配布システムは、電子透かし情報の異なる複数の情報を生成する第1の手段と、上記複数の情報毎に個別の暗号鍵を用いて暗号化して複数の暗号化情報を生成する第2の手段と、上記個別の暗号鍵を別の暗号鍵を用いて暗号化して複数の暗号化暗号鍵を生成する第3の手段と、上記複数の暗号化情報および暗号化暗号鍵をユーザに送信する第4の手段とをサーバが有し、上記送信された複数の暗号化情報や、上記暗号化情報に対応する暗号化暗号鍵の1つを選択する第5の手段をユーザが有する電子情報配付システムにおいて、上記暗号鍵の一部にのみ乱数を乗じるようにする第6の手段をサーバに設けたことを特徴としている。

【0049】また、本発明の電子情報配布システムの他の特徴とするところは、上記サーバは乱数を暗号化して暗号化乱数を生成し、上記暗号化乱数を保存するとともに、ユーザに送信する第7の手段を更に有することを特徴としている。

【0050】また、本発明の電子情報配布システムのその他の特徴とするところは、上記電子透かしの正当性を検証する第8の手段をさらに有することを特徴としている。

【0051】また、本発明の電子情報配布システムのその他の特徴とするところは、上記電子透かしの正当性を検証する処理を繰り返し行うようにしたことを特徴としている。

【0052】また、本発明の電子情報配布システムのその他の特徴とするところは、電子透かし処理により埋め込まれたユーザに対応する電子透かし情報の正当性を暗号化処理を用いて保証するようにした電子情報配付システムにおいて、上記ユーザの電子透かし情報を検査する検査手段を有することを特徴としている。

【0053】また、本発明の電子情報配布システムのその他の特徴とするところは、上記ユーザの署名を認証局による証明書付き匿名公開鍵によって検査する検査手段をさらに有することを特徴としている。

【0054】また、本発明の電子情報配布システムのその他の特徴とするところは、上記暗号化処理及び／または電子透かし埋め込み処理を検査するための検査情報を

ヘッダ部に有する画像フォーマットを用いることを特徴としている。

【0055】また、本発明の記憶媒体は、上記電子透かし方式方法の手順をコンピュータに実行させるためのプログラムを格納したことを特徴としている。

【0056】また、本発明の記憶媒体の他の特徴とするところは、上記電子情報配布システムの各手段としてコンピュータを機能させるためのプログラムを格納したことを特徴としている。

【0057】

【作用】本発明は上記技術手段よりなるので、暗号鍵に乱数を乗じる際に、一部の暗号鍵にのみ乱数が乗じられるので、暗号鍵と乱数の処理を逆にすることが防止され、サーバがユーザに意図した暗号鍵を使用させることができなくなる。

【0058】また、本発明の他の特徴によれば、電子透かしを埋め込むための処理に必要な計算量、及び通信量を従来の方式に比べて減少させることができ、電子透かし方式を実施する効率を大幅に向上させることができる。

【0059】

【発明の実施の形態】以下、図1及び図6を参照して、上記第1の問題点を解決する第1の実施の形態を説明する。本実施の形態の手法は、Uブロックに対して乱数を用いず、Sブロックに対してのみ乱数を用いることによって、サーバがユーザに意図した暗号鍵を使用させることを防止しているものであり、プロトコルは以下のようになる。

【0060】〔埋め込み処理〕まず、図6のフローチャートのステップS61に示したように、サーバが原画像をN個のブロックに分割し、各ブロックを P_n ($n=1, \dots, N$)とする。そして、原画像 P_n を N_s 個 ($N_s < N$)のSブロックと、 N_u 個 ($N_u = N - N_s$)のUブロックに分ける。

【0061】図1では、原画像を4分割してブロック P_1 及び P_2 をSブロックとし、 P_3 及び P_4 をUブロックとしている。また、サーバは暗号鍵 k によってデータ P を暗号化する暗号化手段 $E(k, P)$ を準備する(ユーザは、それに対応する復号手段を持つとする)。

【0062】また、サーバとユーザは独立に $e \cdot d = 1 \pmod{p-1}$ となる変数 e と変数 d を生成する。ただし、 $p = 2q + 1$ (q は素数)であり、サーバは以上のような e と d を $N + N_s$ 組生成し、(e_n, d_n)とおく(ユーザの e と d は e_u, d_u とおく)。

【0063】次に、ステップS62において、サーバはSブロックにユーザ毎に定めたユーザ情報を埋め込む。次に、ステップS63に進み、サーバはUブロックの複製を 2^b 個生成して、「 $0 \sim 2^b - 1$ 」の数値を埋め込む。以降、ブロック P_n に数値 i が埋め込まれた時、それを $P_n(i)$ と表現する。図1では、Sブロックであ

る P_1 、 P_2 にユーザ情報として $\{0, 1\}$ が埋め込まれ、 $b=1$ としてUブロックである P_3 、 P_4 の2個の複製に対して0~1の数値が埋め込まれている。

【0064】次に、ステップS64において、サーバはSブロックの $P_n(i)$ の複製を 2^b 個生成し、各々異なる暗号鍵 k_{nj} ($j=0, \dots, 2^b-1$)で暗号化した $E(k_{nj}, P_n(i))$ と、暗号鍵 k_{nj} に乱数 r_n をかけて e_n で暗号化した $(k_{nj} \cdot r_n)^{e_n}$ をともにユーザに送る。

【0065】さらに、サーバは、ステップS65において、 $N_u \cdot 2^b$ 個のUブロック $P_n(i)$ を各々鍵 k_{ni} で暗号化した $E(k_{ni}, P_n(i))$ と、鍵 k_{ni} を e_n で暗号化した $(k_{ni})^{e_n}$ をともにユーザに送る。また、Sブロックの乱数 r_n を e_n' ($n'=N+n$)で暗号化した $r_n^{e_n'}$ を保存し、かつユーザに送る。以後、 $E(k, P)$ によって暗号化した画像を暗号化画像、暗号鍵を e_u で暗号化したものをサーバ暗号化暗号鍵、また e_n' で暗号化した乱数をサーバ暗号化乱数と呼ぶ。このとき、暗号化画像やサーバ暗号化暗号鍵、サーバ暗号化乱数はその対応が正しければランダムに送ることができる。

【0066】次に、ステップS66において、ユーザは、送られてきた複数の暗号化画像とサーバ暗号化暗号鍵のペアの中から各ブロック毎に1つずつのペアを選ぶ。図1では、各ブロック毎に $E(k_{11}, P_1(0))$ ($k_{11} \cdot r_1$) e_1 、 $E(k_{20}, P_2(1))$ ($k_{20} \cdot r_2$) e_2 、 $E(k_{31}, P_3(1))$ ($k_{31} \cdot r_3$) e_3 、 $E(k_{40}, P_4(0))$ ($k_{40} \cdot r_4$) e_4 を選んだことになる。

【0067】次に、ステップS67において、ユーザは、選んだサーバ暗号化暗号鍵とすべてのサーバ暗号化乱数を自分の暗号鍵 e_u で暗号化して、2重暗号化暗号鍵と2重暗号化乱数を生成してサーバに送る。このとき、ユーザはすべてのサーバ暗号化乱数をつなぎ合わせた合成乱数に対するハッシュ値に公開鍵暗号方式による署名を施してサーバに送る。これは、図1において、 $\text{SigU}(h(r_1^{e_1'} \parallel r_2^{e_2'}))$ で表される。

【0068】次に、ステップS68に示すように、サーバは、ユーザの公開鍵を用いて署名を検査した後、送られてきた2重暗号化暗号鍵と2重暗号化乱数の復号を行う。すなわち、 e_n で暗号化されたデータに対して d_n 乗して mod をとる。

【0069】次に、ステップS69において、サーバは復号した暗号化暗号鍵(ユーザ暗号化暗号鍵)を暗号化乱数(ユーザ暗号化乱数)で割り、その結果をユーザに送る。このとき、サーバは復号したSブロックのユーザ暗号化乱数と、Uブロックのユーザ暗号化暗号鍵と、送られてきた署名を保存する。

【0070】図1では、これによって「 $k_{11}^{e_u}$ 、 $k_{20}^{e_u}$ 、 $k_{31}^{e_u}$ 、 $k_{40}^{e_u}$ 」がユーザに送られ、「 r_1

e_u 、 $r_2^{e_u}$ 、 $k_{31}^{e_u}$ 、 $k_{40}^{e_u}$ 」と、 $\text{SigU}(h(r_1^{e_1'} \parallel r_2^{e_2'} \parallel r_3^{e_3'} \parallel r_4^{e_4'}))$ がサーバに保存される。

【0071】次に、ステップS70において、ユーザは送られてきたユーザ暗号化暗号鍵を復号し、その復号された暗号鍵によって暗号化画像を復号し、分割された各ブロックを合成することによって電子透かし画像を得る。図1では、送られたユーザ暗号化暗号鍵を復号する。すなわち、送られたユーザ暗号化暗号鍵を d_u 乗して mod をとることによって暗号鍵 k_{11} 、 k_{20} 、 k_{31} 、 k_{40} を得ることができる。

【0072】この鍵は、ステップS66で選択した暗号化画像の暗号鍵となっているので、この鍵で暗号化画像を復号することにより、 $P_1(0)$ 、 $P_2(1)$ 、 $P_3(1)$ 、 $P_4(0)$ を得ることができる。

【0073】よって、各ブロックを合成することによりSブロックにユーザ情報 $\{0, 1\}$ を持ち、ユーザによって選択された $\{1, 0\}$ のパターンをUブロックに持つ電子透かし画像が得られる。

【0074】上記のプロトコルに対応する検証処理は、従来技術で説明した第1の検証処理で検証者に送られる署名を $\text{SigU}(h(r_1^{e_1'} \parallel r_2^{e_2'} \parallel r_3^{e_3'} \parallel r_4^{e_4'}))$ から $\text{SigU}(h(r_1^{e_1'} \parallel r_2^{e_2'}))$ 、サーバ暗号化乱数を「 $r_1^{e_1'}$ 、 $r_2^{e_2'}$ 、 $r_3^{e_3'}$ 、 $r_4^{e_4'}$ 」から「 $r_1^{e_1'}$ 、 $r_2^{e_2'}$ 」に変更すれば同様の処理によって実現できることは明らかである。

【0075】これによって、暗号鍵と乱数の処理を逆にすることが防止され、サーバがユーザに意図した暗号鍵を使用させることができなくなる。また、電子透かしを埋め込むための処理に必要な計算量、及び通信量を従来の方式に比べて減少させることができ、電子透かし方式を実施する効率を大幅に向上させることができる。

【0076】また、安全性よりも計算量や通信量の削減や処理の簡単化を行う場合、すべての乱数 r_n に関する処理を省略することもできる。この場合、上記ステップS64において、Sブロックの複製を生成する必要はなく、1つの暗号鍵 k_n による暗号化 $E(k_n, P_n(i))$ と $(k_n)^{e_n}$ を作成すればよい。また、それ以降の乱数 r_n に関するすべての処理を省略することができる。

【0077】〔第2の実施の形態〕以下、上述した第2の問題点を解決するための実施の形態を、図2及び図7を参照して説明する。本実施の形態の手法は、画像分割数 N とUブロックの数 N_u に依存せず、検証処理を繰り返すことによって高い安全性を実現することができる。具体的な検証処理は以下のようになる。

【0078】〔検証処理〕図7に示したように、サーバは、最初のステップS71において、不正画像のSブロックからユーザ情報を取り出し、不正を行ったと思われる

るユーザを推定する。次に、ステップS72に進み、サーバは不正画像に基づいてUブロックにおいてユーザが選択した各々のブロックを特定し、そのブロックを暗号化した暗号鍵を特定する。

【0079】次に、ステップS73に進み、サーバは、特定したユーザ名、及び保存しているSブロックのユーザ暗号化乱数とUブロックのユーザ暗号化暗号鍵と署名、さらに上記埋め込み処理におけるステップS65で保存したすべてのサーバ暗号化乱数と、Sブロックの乱数と、特定したUブロックの暗号鍵を検証者に渡して検証を依頼する。

【0080】よって、図2では、サーバは検証者にユーザ名の他に「 $r1^{eu}$ 、 $r2^{eu}$ 、 $k31^{eu}$ 、 $k40^{eu}$ 、 $SigU(h(r1^{e1'} \parallel r2^{e2'} \parallel r3^{e3'} \parallel r4^{e4'}))$ 、 $r1^{e1'}$ 、 $r2^{e2'}$ 、 $r3^{e3'}$ 、 $r4^{e4'}$ 、 $r1$ 、 $r2$ 、 $k31$ 、 $k40$ 」を送る。

【0081】検証者は、ステップS74において、上記埋め込み処理におけるステップS65で保存されたサーバ暗号化乱数からハッシュ値を生成し、ユーザの公開鍵を用いて署名を検査し、一致するかどうかを検査する。

【0082】この検査の結果、署名が一致したか否かをステップS75において判断する。そして、署名が一致しない場合には、そのサーバ暗号化乱数はそのユーザへの埋め込み処理に用いられたものではないので、ステップS76に進み、ユーザは不正していないと認定する。

【0083】一方、ステップS75の検査結果が一致した場合には、ステップS78に進み、検証者は、上記埋め込み処理で用いられたデータPを基にN組の異なる鍵を生成し、Sブロックの乱数とUブロックの暗号鍵を暗号化し、順番を変えてユーザに送る。

【0084】図2では、4組の暗号鍵（ $e1''$ 、 $d1''$ ）～（ $e4''$ 、 $d4''$ ）が生成され、Sブロックの乱数 $r1$ 、 $r2$ とUブロックの暗号鍵 $k31$ 、 $k40$ を、「 $r1^{e1''}$ 、 $r2^{e2''}$ 、 $k31^{e3''}$ 、 $k40^{e4''}$ 」と暗号化される。

【0085】次に、ステップS78に進み、ユーザは、送られてきたデータを埋め込み処理で用いた暗号鍵 eu によって暗号化してサーバに送る。図2では、「 $r1^{e1'' eu}$ 、 $r2^{e2'' eu}$ 、 $k31^{e3'' eu}$ 、 $k40^{e4'' eu}$ 」がサーバに送られる。ここで、Sブロックの乱数 $r1$ 、 $r2$ とUブロックの暗号鍵 $k31$ 、 $k40$ は順番が変えられているので、ユーザはSブロックとUブロックに属すブロックを識別できない。

【0086】次に、ステップS79において乱数の比較処理を行うとともに、ステップS80において鍵の比較処理を行う。これは、サーバが、送られてきたデータを復号、すなわち、 di'' 乗して mod をとり、その結果を保存されていたSブロックのユーザ暗号化乱数とUブロックのユーザ暗号化暗号鍵とを比較する。

【0087】この比較の結果、Sブロックのユーザ暗号

化乱数が一致しない場合はユーザが埋め込み処理と異なる鍵で上述した埋め込み処理を行ったことになるので、ステップS79からステップS81に進み、ユーザの不正と認定される。

【0088】一方、Sブロックのユーザ暗号化乱数が一致し、Uブロックのユーザ暗号化暗号鍵が一致しない場合はユーザの不正と認定されない。また、Sブロックのユーザ暗号化乱数が一致し、Uブロックのユーザ暗号化暗号鍵が一致した場合もユーザの不正と認定される。よって、図2に示すように、Sブロックのユーザ暗号化乱数「 $r1^{eu}$ 、 $r2^{eu}$ 」とUブロックのユーザ暗号化暗号鍵「 $k31^{eu}$ 、 $k40^{eu}$ 」を比較する。ただし、Sブロックのユーザ暗号化乱数が一致し、Uブロックのユーザ暗号化暗号鍵が一致しない場合はステップS82に進んで所定の回数終了したか否かを判断する。

【0089】サーバは、所定の回数終了したか、または納得が行けば処理を終了し、この場合はユーザの不正が認定されない。そうでない場合、上述した検証処理を繰り返す。以上の検証処理において、不正を行ったユーザが1つのブロックを異なる暗号鍵で暗号化したとすると、 Nu/N の確率で成功する（検証者によってユーザの不正と認定されない）。

【0090】上述した検証処理において、上記ステップS77～ステップS82の処理を k 回繰り返すとすると、不正を行ったユーザは常に同じブロックを異なる暗号鍵で暗号化する必要があるが、ステップS77において、サーバが送るデータは順番が毎回異なるので、ユーザは前回異なる暗号鍵で暗号化したブロックを特定できない。

【0091】よって、本実施の形態の検証処理では、不正を行ったユーザは $(Nu/N)^k$ の確率でしか成功せず、 k の値を大きくすることによって画像の分割に依存せず、検証処理の安全性を高めることができる。

【0092】また、第1の実施の形態の埋め込み処理に本実施の形態の検証処理を適用する場合、本実施の形態の検証処理で検証者に送られる署名を $SigUj(h(r1^{e1'} \parallel r2^{e2'} \parallel r3^{e3'} \parallel r4^{e4'}))$ から、 $SigU(h(r1^{e1'} \parallel r2^{e2'}))$ 、サーバ暗号化乱数を「 $r1^{e1'}$ 、 $r2^{e2'}$ 、 $r3^{e3'}$ 、 $r4^{e4'}$ 」から、「 $r1^{e1'}$ 、 $r2^{e2'}$ 」に変更すれば、同様の処理によって安全性の高い検証処理を実現することができる。

【0093】〔第3の実施の形態〕以下、上記第2の問題点を解決する実施の形態を図3及び図8を参照して詳細に説明する。この手法は、上記第2の実施の形態で示した検証処理のように、暗号的手法を用いずに直接画像を検査することによって検証処理を軽減することができる。

【0094】具体的な手順は、以下のようになる。ただし、埋め込み処理の前にサーバはユーザから画像購入に関する契約情報を入手しているとし、検証者は電子透か

し情報の抽出法を知っているとす。

【0095】〔検証処理〕図8のステップS81に示したように、サーバは、不正画像のSブロックからユーザ情報を取り出し、不正をしたと思われるユーザを推定する。次に、ステップS82に進み、サーバは上記推定した不正画像に基づいて、Uブロックにおいてユーザが選択した各々のブロックを特定し、そのブロックに埋め込んだ数値を特定する。

【0096】次に、ステップS83に進み、サーバは、上記特定したユーザ名、及びそのユーザからの契約情報と、Sブロックに埋め込まれた数値と、Uブロックに埋め込まれた数値を検証者に渡して検証を依頼する。

【0097】よって、図3ではサーバは検証者にユーザ名のほかに、ユーザからの契約情報(SigU(C))と表し、Cはユーザ名などを特定したユーザからの購入希望文書であり、SigU()はそのユーザにより署名がなされていることを表す)と、各ブロックから特定した数値(0、1、1、0)を送っている。

【0098】次に、ステップS84に進み、検証者は、契約情報を確認する。検証者は購入した画像をユーザから提出させる(図3参照)。

【0099】次に、ステップS85において、検証者は、ユーザから提出された画像の各ブロックから埋め込まれた数値を抽出する。そして、次のステップS86において、上記抽出した数値とサーバから示された数値とが一致するかを各ブロック毎に比較する。

【0100】この比較の結果、ユーザ画像から抽出された数値とサーバから提出された数値とが一致した場合にはユーザの不正と認定され、一致しない場合ユーザの不正と認定されない。

【0101】本実施の形態は、従来の方式の埋め込み処理、及び第1、第2の実施の形態の埋め込み処理に対して適用できることは明らかである。さらに、本実施の形態により検証処理を行う場合、埋め込み処理におけるサーバによる暗号化乱数や暗号化暗号鍵の保存や、ユーザによる暗号化乱数のハッシュ値に対する署名の処理を省略できることも明らかである。

【0102】また、検証局は電子透かし情報を抽出できるので、電子透かし情報抽出のための秘密鍵を知り、信頼できる機関である必要があるので、鍵供託システムまたは鍵復元システムにおける鍵管理局とすることも考えられる。

【0103】〔その他の実施の形態〕透かし情報の埋め込みは公知の埋め込み手法によって実現できるが、例えば電子透かしを埋め込み方法の例としては、離散コサイン変換を利用するものとしてNTTの方式(中村、小川、高鳴、"デジタル画像の著作権保護のための周波数領域における電子透かし方式" SCIS-97-26A, 1997年1月)の他に、離散フーリエ変換を利用するものとして防衛大の方式(大西、岡、松井、"PN

系列による画像への透かし署名法" SCIS-9726B, 1997年1月)や、離散ウェーブレット変換を利用するものとして三菱、九大の方式(石塚、坂井、櫻井、"ウェーブレット変換を用いた電子透かし技術の安全性と信頼性に関する実験的考察"、SCIS'1997年1月)などが挙げられる。

【0104】また、暗号処理E(k, P)は、種々の暗号方式によって実現できるが、例えば、DESやFEAL等のような共通鍵暗号方式によって容易に実現することができる。

【0105】また、上述の実施の形態の画像分割は、図1~図3に示したような平面的な分割だけでなく、多値画像における各位に対応するビットプレーンやRGBのような色毎の分割や、合成すれば元の画像に電子透かしが埋め込まれた画像になる分割手法を全て含む。また、原画像となるものは、静止画像に限定されず、動画や音声などすべてのデジタル情報を含むことができる。

【0106】また、上述の実施の形態では不正画像の検出はサーバが行っているが、不正画像の発見者はサーバに限定されず、特定の検査機関や電子透かしの抽出法を知る他者が行うことが可能である。

【0107】また、サーバからの暗号化画像とサーバ暗号化暗号鍵、サーバ暗号化乱数等はネットワークやCD-ROM等によって広く配布されていてもよい。また、暗号化画像に対応するサーバ暗号化暗号鍵、サーバ暗号化乱数にサーバが署名を施し、その対応を保証することも可能である。

【0108】また、埋め込み処理を行う前にユーザからの画像データを要求する契約情報がサーバによせられることが考えられる。このとき、契約情報がユーザの公開鍵暗号方式を用いた署名によって実現されることもある。

【0109】また、その署名を検査する公開鍵が認証局によって保証されていることも考えられる。この場合、その公開鍵とユーザとの関係が認証局によって秘密に保たれれば、ユーザの匿名性を実現することもできる。

【0110】また、サーバとユーザとの間に画像販売の代理を行う代理店があるシステムに用いることも可能である。このとき、埋め込み処理のサーバ暗号化乱数やサーバ暗号化暗号鍵の生成をサーバと代理店とで分担して行ったりすることもできる。

【0111】〔第4の実施の形態〕本発明に示したサーバまたはユーザによる暗号化暗号鍵や暗号化乱数等は、任意の画像フォーマットで格納することができる。特に、一般的な画像フォーマットでは、送付される電子透かし画像データまたは暗号化画像を画像データ部に格納し、その電子透かしに対するサーバまたはユーザによる暗号化暗号鍵や暗号化乱数等を含む種々の情報をヘッダ部に格納することができる。

【0112】一方、下記に示すFlashPixTMフ

ファイルフォーマットでは、上記のようなサーバまたはユーザによる暗号化暗号鍵や暗号化乱数等を含む一般的な画像フォーマットを各階層のデータとして格納することができる。また、サーバまたはユーザによる暗号化暗号鍵や暗号化乱数等は属性情報としてプロパティセットの中に格納しておくこともできる。

【0113】以下、説明するFlashPix™ (FlashPixは米国Eastman Kodak社の登録商標) ファイルフォーマットでは、上記画像ヘッダ部に格納されていた画像属性情報および画像データをさらに構造化してファイル内に格納する。

【0114】上記構造化した画像ファイル内の各プロパティやデータにはMS-DOSのディレクトリとファイルに相当する、ストレージとストリームによってアクセスする。画像データや画像属性情報はストリーム部分に格納される。

【0115】画像データは、異なる解像度で階層化されており、それぞれの解像度の画像をSubimageと呼び、Resolution 0、1...nで示す。各解像度画像に対して、その画像を読み出すために必要な情報がSubimage headerに格納され、また画像データがSubimage dataに格納される。

【0116】ここで、プロパティセットとは、属性情報をその使用目的、内容に応じて分類して定義したもので、Summary Info. Property Set、Image Info Property Set、Image Content Property Set、Extension list property Setがある。

【0117】Summary Info. Property Setは、FlashPix特有のものではなく、Microsoft社のストラクチャードストレージでは必須のプロパティセットで、そのファイルのタイトル・題名・著者・サムネール画像等を格納する。

【0118】Image Contents Property Setは、画像データの格納方法を記述する属性である。この属性には、画像データの階層数、最大解像度の画像の幅及び高さや、それぞれの解像度の画像についての幅、高さ、色の構成、あるいはJPEG圧縮を用いる際の量子化テーブル・ハフマンテーブルの定義を記述する。

【0119】Image Info. Property Setは、画像を使用する際に利用できる様々な情報、例えば、その画像がどのようにして取り込まれ、どのように利用可能であるかの情報を格納する。

【0120】Extension list property Setは、FlashPixの基本仕様には含まれない下記(イ)～(リ)の情報を追加する際に使用する領域である。

(イ) デジタルデータの取り込み方法/あるいは生成方法に関する情報 (File Source)、(ロ) 著作権に関する情報 (Intellectual property)、(ハ) 画像の内容 (画像中の人物、場所など) に関する情報 (Content description)、(ニ) 撮影に使われたカメラに関する情報 (Camera information)、(ホ) 撮影時のカメラのセッティング (露出、シャッタースピード、焦点距離、フラッシュ使用の有無など) の情報 (Per Picture camera settings)、(ヘ) デジタルカメラ特有解像度やモザイクフィルタに関する情報 (Digital camera characterization)、(ト) フィルムのメーカー名、製品名、種類 (ネガ/ポジ、カラー/白黒) などの情報 (Film description)、(チ) オリジナルが書物や印刷物である場合の種類やサイズに関する情報 (Original document scan description)、(リ) スキャン画像の場合、使用したスキャナやソフト、操作した人に関する情報 (Scan device)。

【0121】なお、FlashPixにおいて、FlashPix Image ViewObjectは、画像を表示する際に用いるビューイングパラメータと画像データとを合わせて格納する、画像ファイルである。

【0122】上記ビューイングパラメータとは、画像の回転、拡大/縮小、移動、色変換、フィルタリングの処理を画像表示の際に適応させるために記憶しておく処理係数のセットである。

【0123】Source/Result FlashPix Image Objectは、FlashPix画像データの実体であり、Source FlashPix Image Objectは必須であり、Result FlashPix Image Objectはオプションである。

【0124】Source FlashPix Image Objectは、オリジナルの画像データを、Result FlashPix Image Objectはビューイングパラメータを使って画像処理した結果の画像を格納する。

【0125】Source/Result desc. Property setは上記画像データの識別のためのプロパティセットであり、画像ID、変更禁止のプロパティセット、最終更新日時等を格納する。

【0126】Transform property setは回転、拡大/縮小、移動のためのAffine変換係数、色変換マトリクス、コントラスト調整値、フィルタリング係数を格納している。

【0127】また、上記実施の形態におけるハッシュ値、認証局、公開鍵暗号方式、共通鍵暗号方式を、以下

にまとめて説明する。すなわち、ハッシュ値とは、ハッシュ関数 h の出力値であり、ハッシュ関数とは衝突を起こしにくい圧縮関数をいう。ここで、衝突とは異なる x_1 、 x_2 に対して $h(x_1) = h(x_2)$ となることである。

【0128】また、圧縮関数とは、任意のビット長のビット列をある長さのビット列に変換する関数である。したがって、ハッシュ関数とは任意のビット長のビット列をある長さのビット列に変換する関数であり、 $h(x_1) = h(x_2)$ を満たす x_1 、 x_2 を容易に見出せないものである。

【0129】このとき、任意の y から $y = h(x)$ を満たす x を容易に見出せないで、必然的にハッシュ関数は一方向性関数となる。ハッシュ関数の具体例としては、MD(Message Digest)5や、SHA(Secure Hash Algorithm)等が知られている。

【0130】〔認証局〕公開鍵暗号方式におけるユーザの公開鍵の正当性を保証するために、ユーザの公開鍵に証明書を発行する機関を認証局と言う。すなわち、ユーザの公開鍵やユーザに関するデータに認証局の秘密鍵で署名を施すことによって証明書を作成して発行する。

【0131】例えば、あるユーザから自分の証明書付き公開鍵を送られたユーザは、この証明書を認証局の公開鍵で検査することによって、公開鍵を送ってきたユーザの正当性(少なくとも、認証局によって認められたユーザであるということ)を認証する。このような認証局を運営している組織としてVeriSignや、CyberTrustという企業がよく知られている。

【0132】〔公開鍵暗号方式〕公開鍵暗号方式は、暗号鍵と復号鍵とが異なり、暗号鍵を公開にし、復号鍵を秘密に保持するようにしている暗号方式である。

【0133】代表例として、RSA暗号やElGamal暗号等が知られている。以下の(1)～(3)のような特徴をもち、秘密通信や認証通信等を実現することができる。

(1) 暗号鍵と復号鍵とが異なり、暗号鍵を公開できるように暗号鍵を秘密に配送する必要がなく、鍵配送が容易である。

【0134】(2) 各利用者の暗号鍵は公開されているので、利用者は各自の復号鍵のみを秘密に記憶しておけばよい。

【0135】(3) 送られてきた通信文の送信者が偽者でないこと、及びその通信文が改ざんされていないことを受信者が確認するための認証機能を実現できる。

【0136】〔鍵供託システムまたは鍵復元システム〕鍵供託システムまたは鍵復元システムとは、暗号鍵を信頼できる第3者に預けて、犯罪や鍵紛失等が起こった場合に、その第3者から暗号鍵の入手が可能になっているシステムをいう。

【0137】(本発明の他の実施形態)本発明は複数の機器(例えば、ホストコンピュータ、インタフェース機器、リーダ、プリンタ等)から構成されるシステムに適用しても1つの機器からなる装置に適用しても良い。

【0138】また、上述した実施形態の機能を実現するように各種のデバイスを動作させるように、上記各種デバイスと接続された装置あるいはシステム内のコンピュータに対し、上記実施形態の機能を実現するためのソフトウェアのプログラムコードを供給し、そのシステムあるいは装置のコンピュータ(CPUあるいはMPU)に格納されたプログラムに従って上記各種デバイスを動作させることによって実施したものも、本発明の範疇に含まれる。

【0139】また、この場合、上記ソフトウェアのプログラムコード自体が上述した実施形態の機能を実現することになり、そのプログラムコード自体、およびそのプログラムコードをコンピュータに供給するための手段、例えばかかるプログラムコードを格納した記憶媒体は本発明を構成する。かかるプログラムコードを記憶する記憶媒体としては、例えばフロッピーディスク、ハードディスク、光ディスク、光磁気ディスク、CD-ROM、磁気テープ、不揮発性のメモ리카ード、ROM等を用いることができる。

【0140】また、コンピュータが供給されたプログラムコードを実行することにより、上述の実施形態の機能が実現されるだけでなく、そのプログラムコードがコンピュータにおいて稼働しているOS(オペレーティングシステム)あるいは他のアプリケーションソフト等の共同して上述の実施形態の機能が実現される場合にもかかるプログラムコードは本発明の実施形態に含まれることは言うまでもない。

【0141】さらに、供給されたプログラムコードがコンピュータの機能拡張ボードやコンピュータに接続された機能拡張ユニットに備わるメモリに格納された後、そのプログラムコードの指示に基づいてその機能拡張ボードや機能拡張ユニットに備わるCPU等が実際の処理の一部または全部を行い、その処理によって上述した実施形態の機能が実現される場合にも本発明に含まれることは言うまでもない。

【0142】

【発明の効果】上述の説明から明らかなように、本発明によれば、暗号鍵に乱数を乗じる際に、一部の暗号鍵にのみ乱数が乗じられるので、暗号鍵と乱数の処理を逆にするのを防止することができる。これにより、サーバがユーザに意図した暗号鍵を使用させないようにすることができ、サーバが利用者情報を勝手に埋め込みそのコピーを不正に配布することを防止することができる。

【0143】また、本発明の他の特徴によれば、電子透かしを埋め込むための処理に必要な計算量、及び通信量を従来の方式に比べて減少させることができ、電子透かし

し方式を実施する効率を大幅に向上させることができ、デジタルデータの不正配布に関して安全で高効率なシステムを実現することができる。

【図面の簡単な説明】

【図1】第1の実施の形態に示した埋め込み処理を説明するための図である。

【図2】第2の実施の形態に示した検証処理を説明するための図である。

【図3】第3の実施の形態に示した検証処理を説明するための図である。

【図4】従来の埋め込み処理を説明するための図である。

【図5】従来の検証処理を説明するための図である。

【図6】第1の実施の形態に示した埋め込み処理の手順を説明するためのフローチャートである。

【図7】第2の実施の形態に示した検証処理の手順を説明するためのフローチャートである。

【図8】第3の実施の形態に示した検証処理の手順を説明するためのフローチャートである。

【符号の説明】

P1, P2, P3, P4 ブロック画像

k 暗号鍵

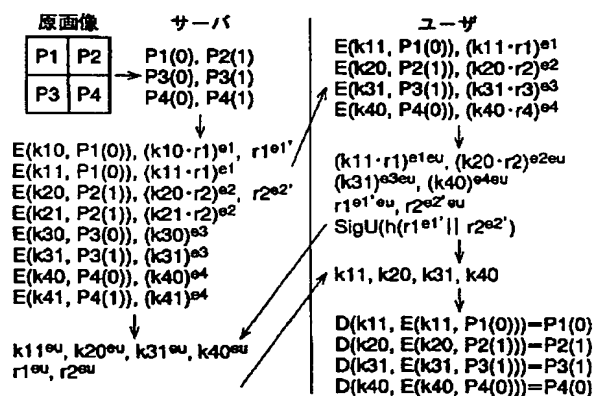
E(k, P) 暗号化手段

e サーバ暗号鍵

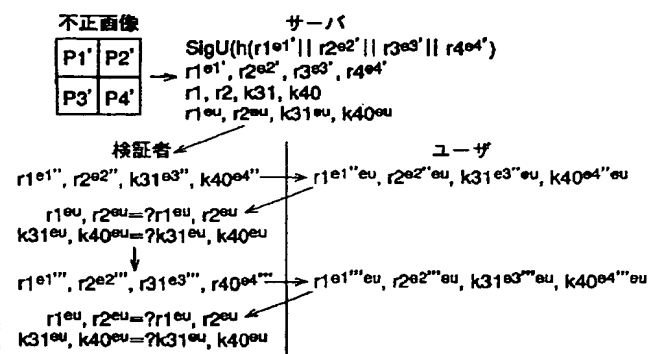
eu ユーザ暗号鍵

SigU 署名

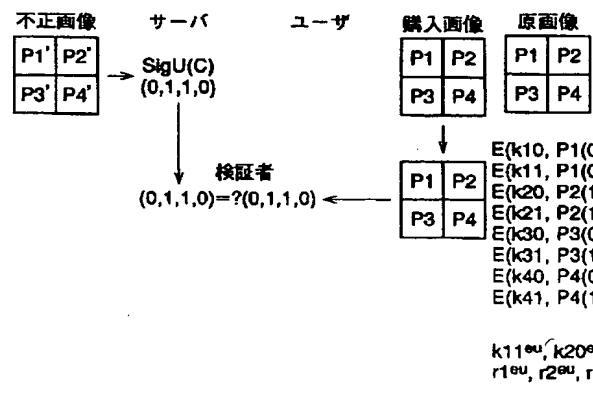
【図1】



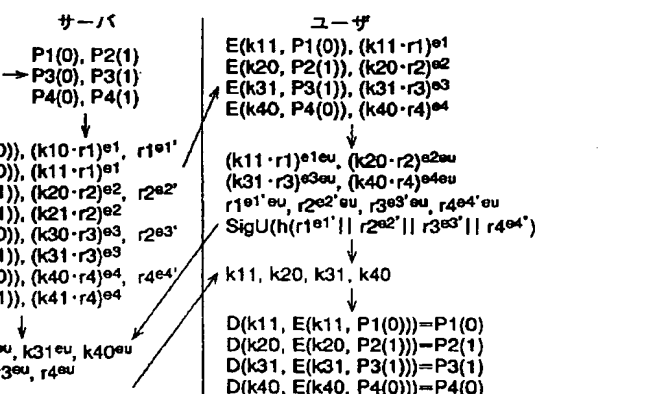
【図2】



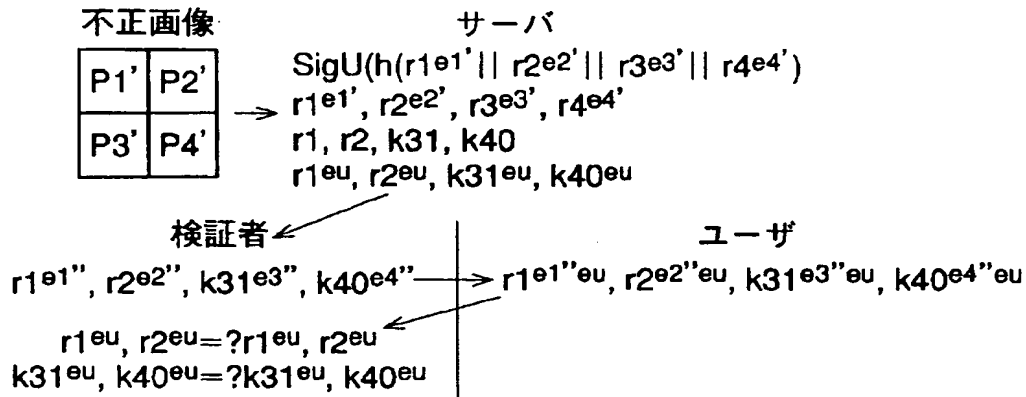
【図3】



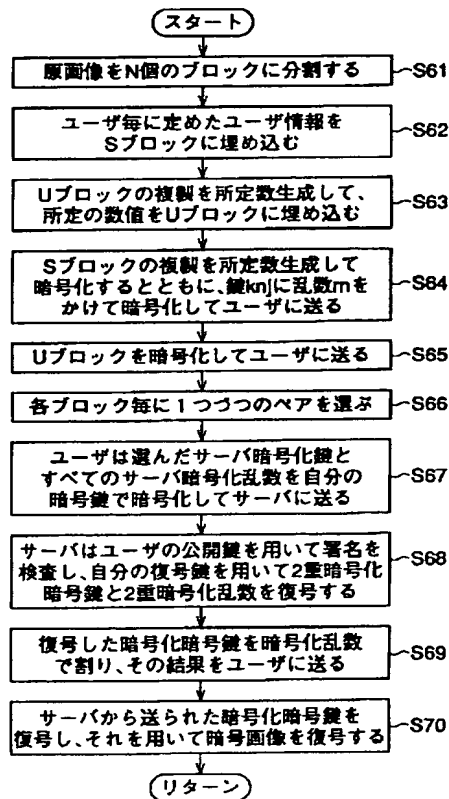
【図4】



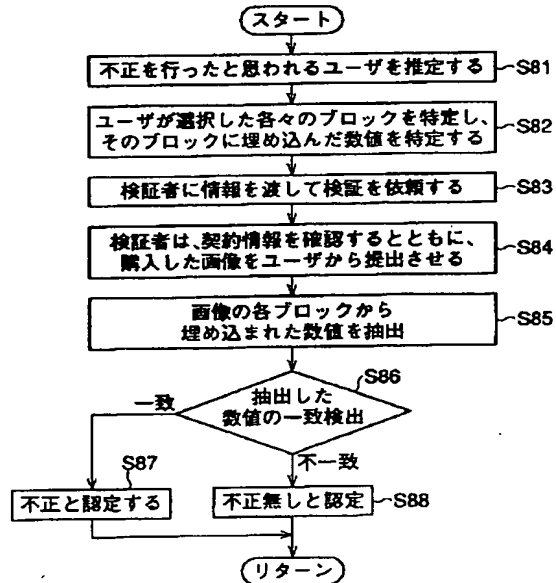
【図5】



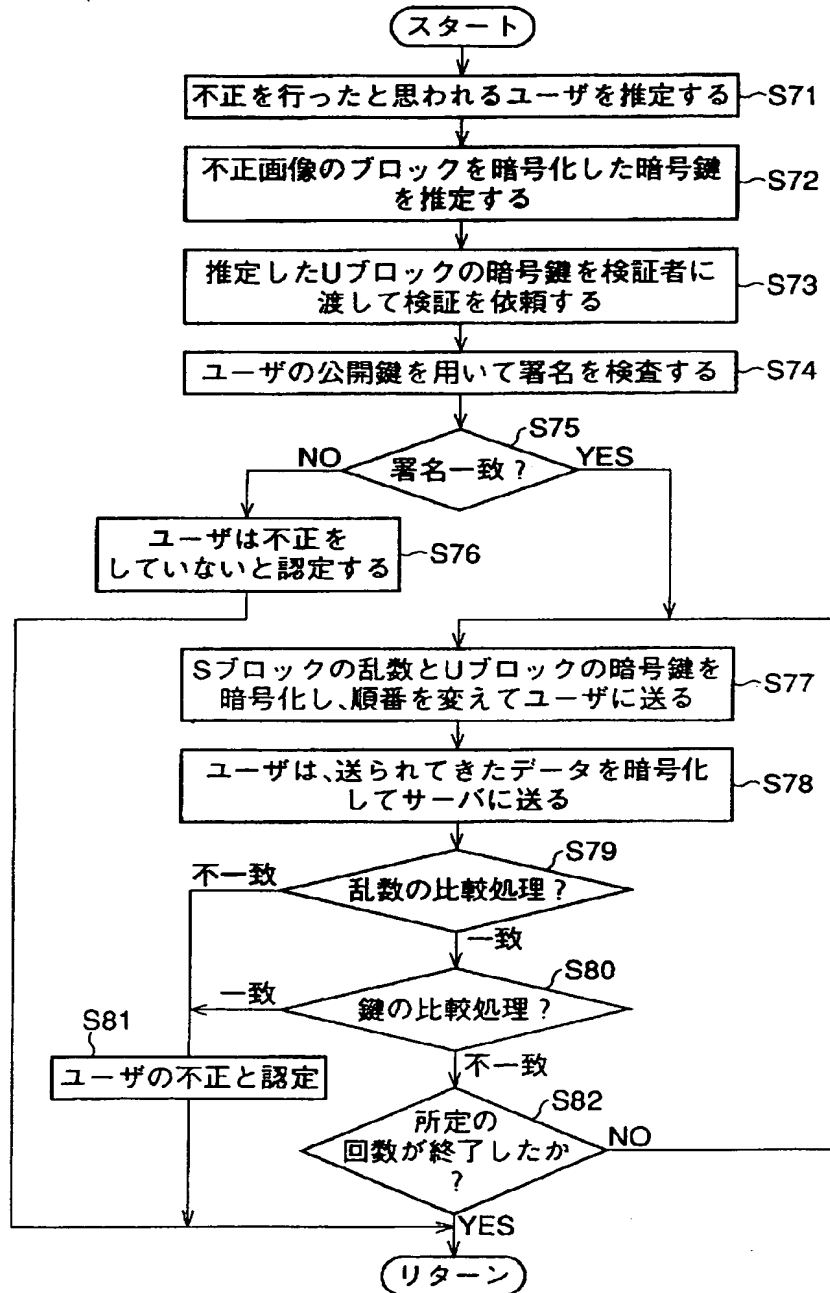
【図6】



【図8】



【図7】



フロントページの続き

(51)Int. Cl.⁶H04N 5/91
7/08

識別記号

FI

H04N 5/91
7/08P
Z

(15)

特開平11-234264

7/081